Policy Title And ID number	**Data Protection Policy** **ID Code: GEN 6.42**			
Sponsoring Director:	**Director of Quality and Standards**			
Implementation Lead:	**Information Governance Manager**			
Impact:	*(a) To patients*			
	(b) To Staff	✓		
	(c) Financial			
	(d) Equality Impact Assessment (EIA)	Completed: **Yes / No** *(delete as applicable)*		
	(e) Other			
Additional Costs:			*Budget Code*	*Revenue or Non Revenue*
	(a) Training:	£ -		
	(b) Implementation:	£ -		
	(c) Capital:	£ -		
	(d) Other	£ -		
Training implications:	*To be incorporated into induction:* **No**		*Other:*	
Date of consultation at:	*Board of Directors*		For Note: January 2011	
	Executive Team			
	Divisional Medical Directors/Clinical Directors			
	Assistant Divisional Directors/Heads of Department			
	Non-Clinical Governance and Risk Committee		*7th December 2010*	
	Joint Partnership Forum		*14th December 2010*	
	Local Negotiating Committee		*N/A*	
	Infection Control Committee:		*N/A*	
	Health & Safety Committee		*N/A*	
	Other (state name/s):		*IGG Group 28th October 2010*	
Alignment	*HR:*		✓	
	Strategic Direction:			
	Board Assurance:			
	Clinical Governance:			
Date of Final Draft:	***December 2010***		Issue Number:	2
Date of Final Approval:	*January 2011*		Approved by:	
Implementation Date:	*February 2011*			
Date of last review:	Nov 2005	Date of next review:	Dec 2012	
Circulation Date:				
Circulation:			Yes	Comment
	Directors		Yes	
	Non Executive Directors		Yes	
	Divisional Medical Directors/Clinical Directors		Yes	
	Medical Staff Committee/SMSF		Yes	
	Assistant Divisional Directors		Yes	
	Assistant Nursing Directors		Yes	
	Heads of Department		Yes	
	H&S Committee Members		Yes	
	Policy database/warehouse		Yes	
	Others (to be listed):		All Trust Staff	

Barnsley Hospital NHS
NHS Foundation Trust

Data Protection Policy

Data Protection Policy

Introduction

Barnsley Hospital NHS Foundation Trust (BHNFT) has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT security. It also has a duty to comply with guidance issued by the Department of Health, the Information Commissioner, other advisory groups to the NHS and guidance issued by professional bodies.

1 Aim

This Data Protection Policy details how BHNFT will meet its obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the policy are primarily based upon the Data Protection Act 1998 as that is the key piece of legislation covering security and confidentiality of personal information.

2 Legislation

For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. The legislation listed below also refers to issues of security and or confidentiality of personal identifiable information/data:

- Data Protection Act 1998
- Access to Health Records 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice and Immigration Act 2008

3 NHS & Related Guidance

The following are the main publications referring to security and/or confidentiality of personal identifiable information/data (see section A for more information):

- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Information Security: NHS Code of Practice
- Employee Code of Practice (Information Commissioner)

4 Responsibilities

The implementation of, and compliance with, this policy is delegated to the Data Protection Lead who will report to the Information Governance Steering Group who will have responsibility for bringing data protection issues to the Trust Board.

The Data Protection Lead role includes:

- Maintaining registrations
- Facilitating training sessions
- Dealing with subject access requests

- Acting as initial point of contact for any data protection issues which may arise within BHNFT
- Being an active member of the Information Governance Steering Group
- Providing reports to the BHNFT Executive Team as required.
- Auditing data protection compliance
- Facilitating action in areas identified as being non-compliant
- Assisting with complaints concerning data protection breaches
- Acting as the interface between data protection and freedom of information

This policy will be reviewed annually, or more frequently if appropriate, to take into account changes to legislation that may occur, and/or guidance from the Department of Health, the Information Commissioner or any relevant case law.

5 Security & Confidentiality

All information relating to identifiable individuals and any information that may be deemed sensitive, must be kept secure at all times. BHNFT will ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

6 Database Management

The Trust has developed a major Information Asset Register detailing ownership and accountability of all its major systems to ensure that appropriate protection is maintained.

7 Back-ups

Trust servers are backed up at hourly, nightly and weekly intervals using the Netapp SAN snapshot technology. Snapshots are written to tape and the tapes are consequently stored in a fireproof safe within the ICT department.

8 Disclosure of Information & Information in Transit

It is important that information about identifiable individuals (such as the general public, patients and/or staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations.

All disclosures of computer held identifiable information should be included in the relevant data protection registration document for the database the disclosure may be made from.

Some disclosures of information may occur because there is a statutory requirement upon BHNFT to disclose e.g. with a court order, because other legislation requires disclosure (for staff to the tax office, pension agency and for patients to the Department of Health if the patient has a notifiable disease).

If person identifiable information /records needs to be transported in any media such as: disc, memory stick or manual paper records, this should be carried out to maintain strict security and confidentiality of this information. For further information on transporting, sending and receiving person identifiable data please refer to the BHNFT Safe Haven Policy.

Contracts between BHNFT and third parties must include an appropriate confidentiality clause that must be disseminated to the third parties employees.

9 Disclosure of Information Outside the EEA

Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the European Economic Area to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

In the event that any member of staff wishes to process personal information outside of the United Kingdom, the Data Protection Lead must be consulted prior to any agreement to transfer or process information.

10 Training

The Data Protection Lead has overall responsibility for maintaining awareness of confidentiality and security issues for all staff. This is carried out the IG Training Tool (CFH) and identified as a mandatory training requirement through the Trusts Corporate Curriculum.

11 Contracts of Employment

Staff contracts of employment are produced and monitored by BHNFT Human Resources department. All contracts of employment include a data protection and general confidentiality clause. Agency and non-contract staff working on behalf of BHNFT must be subject to the same rules.

All BHNFT employees will be made aware of their responsibilities in connection with the Acts mentioned in this Policy through their Statement of Terms and Conditions, and targeted mandatory training sessions.

12 Disciplinary

A breach of the Data Protection requirements could result in a member of staff facing disciplinary action. A copy of the BHNFT Disciplinary procedure is available on the Human Resources internal website.

13 Monitoring & Audit

This policy will be monitored by the Information Governance Steering Group on a regular basis. In addition, application of this Policy will also be reviewed by Internal and external audit.

14 Subject Access Requests

Current Data Protection legislation allows an individual who is the subject of personal information processed by BHNFT to access their information. In the event that an individual wishes to have a copy of their information under the Subject Access provision of the Data Protection Act a request must be made in writing to the Data Protection Lead.

BHNFT is obliged to respond to requests promptly within 40 calendar days of a request being made for access to records containing person identifiable information. Failure to do so is a breach of the Act and could lead to a complaint to the Information Commissioner. If it is anticipated that a request will take longer than the 40 day period, BHNFT will inform the applicant giving an explanation of the delay and agree a new deadline.

In addition BHNFT will charge for any subject access requests made in line with legislative guidelines.

15 Disclosure of Personal Information

There are Acts of Parliament that govern the disclosure of personal information. Some of these Acts make it a legal requirement to disclose and others that state that information cannot be disclosed. These Acts are detailed below:

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS SHA's from Schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976

In the event that a request for disclosure is made referencing any of these Acts the BHNFT Data Protection Lead must be notified prior to any information being released.

16 Prevention and detection of fraud

In accordance with data protection and human rights legislation, all staff should be aware that their personal data may be used by the Trust for the prevention and detection of fraud. Further information is available within the Trust's Fraud Policy and any queries regarding this work should be referred to the Local Counter Fraud Specialist.

Appendix A

Data Protection Principles

There are 8 principles which must be applied when handling or processing information. These principles form the backbone to the Data Protection Act.

1. Information must be processed fairly and lawfully
2. Information must be processed for the specific purpose or purposes given
3. The information being processed is adequate, relevant and not excessive
4. That information is accurate
5. Information should be kept no longer than is necessary
6. Information is processed in accordance with the subject's rights
7. Information is kept secure at all times
8. Information is not transferred to countries or territories outside the EEA or to countries or territories without adequate protection unless Safe harbour or similar agreements are in place and in operation

Appendix B

Caldicott Principles

The Caldicott Standards are based on the Data Protection Act 1998 principles and again are set out in the form of Principles

The Caldicott Guardian for the Trust is the Medical Director.

Principle 1: **Justify the Purpose**
Every proposed use or transfer of patient-identifiable Information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate Guardian.

Principle 2: **Don't use Patient-Identifiable Information unless it is absolutely necessary**
Patient-identifiable information items should not be used unless there is no alternative

Principle 3: **Use the minimum necessary Patient-Identifiable Information**
Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability

Principle 4: **Access to Patient-Identifiable Information should be on a strict need-to-know basis**
Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see

Principle 5: **Everyone should be aware of their responsibilities**
Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect patient confidentiality

Principle 6: **Understand and Comply with the Law**
Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements